UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/507,190	09/09/2004	Pim Theo Tuyls	NL 020192	1803

24737 7590 08/08/2007

PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
TRAORE, FATOUMATA	
ART UNIT	**PAPER NUMBER**
2136	

MAIL DATE	DELIVERY MODE
08/08/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/507,190	TUYLS ET AL.	
	Examiner	Art Unit	
	Fatoumata Traore	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 June 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3 and 9-19* is/are rejected.

7)☒ Claim(s) *4-8 and 20* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 September 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's amendment filed on June 7, 2007 has been entered. Claims 1-20 are pending in the application. Claims 16 and 19 are amended. Claim 20 is newly added.

Specification

2. Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 17 and 18 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 17 reads the limitation of " A device (P) arranged to operate as the first party and/or as the second party" It is unclear to the examiner if the device is arranged to operate as the first party **and** the second party there will be no need to exchange a key between the same device.

Response to Argument

5. The rejection of claims 1-19 under 35 U.S.C. 101 has been withdrawn in view of applicant argument.

Claim Objections

6. Claims 16-19 were previously objected. The objection of claims 16 and 19 are moot in view of the amendment but the objection to claims 17 and 18 are maintained. Claim 17 is a device claim, which refers back to a system claim. The claims are of different statutory classes; therefore the examiner will examine claims 17 and 18 as system claims.

Response to Amendment

7. Applicant's arguments with respect to claims 1-20 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1, 16, 17, 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Leighton et al** (US 5519778) in view of **Hoffstein et al** (US 6076163).

Claims 1, 16, 17, 19: **Leighton et al** discloses a method, a system, a device, and a computer program product for of generating a private pair of key for enciphering communication between the users comprising:

A first party and a second party, in which the first party holds a value PI and a symmetrical polynomial P (x,y) fixed in the first argument by the value p1, and the first party performs the steps of sending the value p1 to the second party(the individual secret keys allow two users I and j to easily agree on a common secret key Kij namely Kij = F(I, j). Pi and Qi constitute the secret of chip I) (column 4, lines 43-65), receiving a value P2 from the second party and calculating the common secret S1 by evaluating the polynomial P(p1, y) in P2, characterized in that the first party additionally holds a value q1 and a symmetrical polynomial Q(x, z) fixed in the first argument by the value q1(this value is computed by user I evaluating the secret polynomial Pi at point j, and it is computed by user j

evaluating the secret polynomial at Qj at point I) (column 4, lines 24-31 lines 43-65 , column 5 lines 5 lines 14-40 Figs. 1-3), but does not explicitly discloses the steps of sending q1 to the second party, receiving a value q2 from the second party and calculating the secret $1 as SI=Q(ql, q2).P(Pl, P2). However, **Hoffstein et al** discloses a secure user identification method, system, device and computer program product, which further discloses a step of sending q1 to the second party (Fig. 3), a step of receiving a value 2 from the second party (Fig. 3) and a step of calculating the secret S1(column 3, lines 31-46 and Fig. 3). Therefore, it would have been obvious to one having ordinary skills in the art at the time the invention was made to use a challenge response type of authentication in **Leighton et al**'s disclosure. On would have been motivated to do so in order to maintain a secure communication by not allowing eavesdroppers to access critical information.

10. Claims 2, 3, 9-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Leighton et al** (US 5519778) in view of **Hoffstein et al** (US 6076163) in further view of **Matyas et al** (US 5953420).

Claim 2: **Leighton et al** and **Hoffstein et al** disclose a method for of generating a private pair of key for enciphering communication between the users as in claim 1 above, while neither of them exclusive discloses a step of generating random numbers. However, **Matyas et al** discloses a method for establishing an

authenticated shared secret value between a pair of users, which further discloses that the first party further performs the steps of obtaining a random number r1 (user A generates a secret value X1a using a pseudorandom number generator) (column 6, lines 15-20), calculating r1. q1 (generates a public value Y1 from the secret value X1 as Y1 = G^x1 mod p) (column 6 lines 20-25), sending r1.q1 to the second party(each party transmits its own public value Y1 to the other party) (column 6, lines 35-38), receiving r2.q2 from the second party and calculating the secret S1 as S1=Q(q1, r1.r2.q2).P (p1, p2) (each party generates a value Z2 from the public value Y2 received from the other party and its own secret value X2 as Z2 =Y2^x2 mod p) (column 7, lines 33-45). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of **Leighton et al** and **Hoffstein et al** such that the generate random number in the secret key exchange protocol as taught by **Matyas et al**. The motivation of doing so would have been against attempts to retrieve the key.

Claim 3: **Leighton et al**, **Hoffstein et al** and **Matyas et** disclose a method for of generating a private pair of key for enciphering communication between the users as in claim 2 above, and **Matyas et al** further discloses that the first party holds the value q1 multiplied by an arbitrarily chosen value r (user A generates a secret value X1a using a pseudorandom number generator) (column 6, lines 15-20), and the product Q (q1, z). P (p1, y) instead of the individual polynomials P

(p1, y) and Q (q1, z) (generates a public value Y1 from the secret value X1 as Y1 = G^x1 mod p) (column 6 lines 20-25), and the first party performs the steps of calculating r1.r.q1, sending r1.r.q1 to the second party, receiving r2.r.q2 from the second party and calculating the secret S1 as S1= Q (q1, r1.r2.r.q2). P (p1, p2) (each party generates a value Z2 from the public value Y2 received from the other party and its own secret value X2 as Z2 =Y2^x2 mod p) (column 7, lines 33-45). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of **Leighton et al** and **Hoffstein et al** such that the generate random number in the secret key exchange protocol as taught by **Matyas et al**. The motivation of doing so would have been against attempts to retrieve the key.

Claim 9: **Leighton et al** and **Hoffstein et al** disclose a method for of generating a private pair of key for enciphering communication between the users as in claim 1 above, and **Leighton et al** further discloses that the first party and the second party use a non-linear function on the generated secret $1 and $2, respectively, before using it as a secret key in further communications (n fact, the individual secret key assigned by T to user i consists of the two univariate polynomials P.sub.i =P.sub.i (y)=F(i,y) and Q.sub.i =Q.sub.i (x) =F(x,i). P.sub.i and Q.sub.i constitute the secret key of chip I) (column 4, lines 49-55).

Claim 10: **Leighton et al** and **Hoffstein et al** disclose a method for of generating a private pair of key for enciphering communication between the users as in claim 9 above, and **Hoffstein et al** further discloses that a one-way hash function is applied to the generated secrets $1 and $2(the above described user identification technique can be converted to a digital signature technique by the prover applying a one way hash function to Ag(x) to generate a simulated challenge polynomial) (column 3, lines 30-46). Therefore, it would have been obvious to one having ordinary skills in the art at the time the invention was made to use a hash function in **Leighton et al**'s disclosure. On would have been motivated to do so in order to maintain a secure communication by not allowing eavesdroppers to access critical information.

Claim 11: **Leighton et al** and **Hoffstein et al** disclose a method for of generating a private pair of key for enciphering communication between the users as in claim 9 above, and **Leighton et al** further discloses that the first party and the second party use a non-linear function on the generated secret $1 and $2, respectively, before using it as a secret key in further communications (n fact, the individual secret key assigned by T to user i consists of the two univariate polynomials P.sub.i =P.sub.i (y)=F(i,y) and Q.sub.i =Q.sub.i (x) =F(x,i). P.sub.i and Q.sub.i constitute the secret key of chip I) (column 4, lines 49-55).

Claim 12: **Leighton et al** and **Hoffstein et al** disclose a method for of generating a private pair of key for enciphering communication between the users as in claim 1 above, and **Hoffstein et al** further discloses that a step of verifying that the second party knows the secret S1 (Fig. 3). (column 4, lines 49-55). Therefore, it would have been obvious to one having ordinary skills in the art at the time the invention was made to include a step of verifying that the second party knows the secret key in **Leighton et al**'s disclosure. On would have been motivated to do so in order to authenticate the users.

11. Claims 13-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Leighton et al** (US 5519778) in view of **Hoffstein et al** (US 6076163) in further view of **Menezes et al** (handbook of applied Cryptography, ISBN 0-8493-8523-7 1997).

Claim 13: **Leighton et al** and **Hoffstein et al** disclose a method for of generating a private pair of key for enciphering communication between the users as in claim 12 above, while neither of them explicitly a step of applying a zero knowledge protocol. However, **Menezes et al** discloses a similar method, which further discloses that the first party subsequently applies a zero-knowledge protocol to verify that the second party knows the secret S1 (The prover claiming to be A selects a random element from pre-defined set as its secret commitment, and from this computes an associated (public) witness. This provides initial randomness for variation from other protocols runs, and essentially defines a set

of questions all of which the prove claims to be able to answer, thereby a priori constraining her forthcoming response. By protocol design, only the legitimate party A, with knowledge of A's secret, is truly capable of answering all the questions, and the answer to any one of these provides no information about A's long-term secret) (pages 409-410, section (IV)). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of **Leighton et al** and **Hoffstein et al** such that to use a zero-knowledge protocol as taught by **Menezes et al**. The motivation of doing so would have been providing unconditional security.

Claim 14:**Leighton et al** and **Hoffstein et al** disclose a method for of generating a private pair of key for enciphering communication between the users as in claim 12 above, while neither of them explicitly a step of applying a commitment-based protocol and **Menezes et al** disclose a similar method, which further discloses that the first party subsequently applies a commitment-based protocol to verify that the second party knows the secret S1 (The prover claiming to be A selects a random element from pre-defined set as its secret commitment, and from this computes an associated (public) witness. This provides initial randomness for variation from other protocols runs, and essentially defines a set of questions all of which the prove claims to be able to answer, thereby a priori constraining her forthcoming response. By protocol design, only the legitimate party A, with knowledge of A's secret, is truly capable of answering all the

questions, and the answer to any one of these provides no information about A's long-term secret) (pages 409-410, section (IV)). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of **Leighton et al** and **Hoffstein et al** such that to use a commitment based protocol as taught by **Menezes et al**. The motivation of doing so would have been providing unconditional security.

Claim 15: **Leighton et al** and **Hoffstein et al** disclose a method for generating a private pair of key for enciphering communication between the users as in claim 14 above, while neither of them explicitly a step of using a symmetric cipher to encrypt a random challenge. However, **Menezes et al** disclose a similar method which, further discloses that the second party uses a symmetric cipher to encrypt a random challenge (b chooses a random r, computes the witness x = h(r) (x demonstrates knowledge of r without disclosing it and computes the challenge e = PA(r, B)) (page 404, section (I)), and sends the encrypted random challenge to the first party(B sends the encrypted random challenge to A. A decrypts e to recover r' and B' computes x' = h (r') (page 404, section (I) and the first party subsequently uses the same symmetric cipher as a commit function to commit himself to a decryption of the encrypted random challenge (A sends r= r' to B. B succeeds with unilateral entity authentication of A upon verifying) (page 404, section (I)). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of

Leighton et al and **Hoffstein et al** such that to use a symmetric cipher as taught by **Menezes et al**. The motivation of doing so would have been providing unconditional security.

12. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Leighton et al** (US 5519778) in view of **Hoffstein et al** (US 6076163) and in further view of **Oishi** (US 6298153).

Claim 18: **Leighton et al** and **Hoffstein et al** disclose a system for of generating a private pair of key for enciphering communication between the users as in claim 17 above, while neither reference explicitly discloses comprising storage means (303) for storing the polynomial P and the polynomial Q in the form their respective coefficients. However **Oishi** disclose a similar system, which further discloses a storage means (figure 3). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined system of **Leighton et al** and **Hoffstein et al** such that to include a storage means as taught by **Oishi**. The motivation of doing so would have been maintaining data integrity.

Allowable Subject Matter

13. Claims 4-8, 20 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:00 a.m. to 4:00 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar G. Moazzami, can be reached on (571) 272 4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 270-2685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

FT
Friday August 3, 2007

Nassar G. Moazzami
Supervisory Patent Examiner

8/6/07